UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

APR 4 2005

OFFICE OF
WATER

MEMORANDUM

SUBJECT: Policy to Manage Access to Sensitive Drinking Water-Related Information

FROM: Michael H. Shapiro
Deputy Assistant Administrator

TO: Deputy Regional Administrators
Regions 1-10

The Office of Water (OW) is establishing a policy, described below, to more effectively protect sensitive drinking water-related information that the Environmental Protection Agency (EPA) manages. In part, this policy is in response to data handling concerns raised by our stakeholders. In addition, the policy mirrors Agency efforts prior to and since September 11, 2001, to provide protections to sensitive information consistent with federal law, striking the right balance between providing the public free access to information yet protecting it against potential misuse by terrorists or others wishing to do harm.

Purpose

This Office of Water policy will apply appropriate security controls to EPA's receipt, storage, use of, and access to sensitive drinking water program data and provide guidance on how we should interact with states and others regarding these data. We have discussed this policy with the EPA programs and other federal agencies who routinely use drinking water data and they have agreed to follow this policy. We have worked with the Office of Environmental Information (OEI) to ensure that this policy is consistent with federal information categorization standards and the Agency-wide sensitivity criteria. It is imperative that EPA programs, other Federal partners, and State co-regulators have the best available data for program planning and implementation purposes, while ensuring that dissemination of these data comports with national security concerns.

Background

In 1995, EPA was identified as one of six key federal agencies with roles in counterterrorism. Since then, EPA's homeland security infrastructure protection roles have been reaffirmed and expanded in two Presidential Directives (PD) 62 and 63, and the more recent homeland security presidential directives (HSPD). Under HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, EPA has been designated as the Sector-Specific

Agency (SSA) for the drinking water and wastewater critical infrastructure sector. EPA collaborates with federal, state, and local government agencies, as well as private organizations, relevant to protecting the water sector's infrastructure, facilitating vulnerability assessments, and fostering risk management strategies for the water sector. These functions are logical extensions of the activities EPA has undertaken to protect drinking water, surface water, and ground water from contamination over the last three decades.

In 1998, a group of large water systems requested that we control and monitor release of data on latitude and longitude of public water system facilities because of their concern about misuse of these data for harmful purposes. Since September 2001, states, utilities and others have requested guidance from EPA on how to deal with the competing interests between public availability of drinking water information and prudent restrictions on access in the interests of homeland security. After September 11, we continued to control access to the information on latitude and longitude of public water system facilities. In December 2001, OW issued a memorandum to the regions describing how to meet public access requirements for Consumer Confidence Reports and Source Water Assessments while providing adequate security safeguards.

In 2001 and 2002, OW participated in an Agency-wide workgroup, chaired by the Office of Environmental Information (OEI), that conducted two sensitivity reviews of EPA's publicly available information holdings. The second review was triggered by a March 17, 2002, memorandum from White House Chief of Staff Andrew Card, requesting all agencies to re-evaluate sensitive but unclassified information to determine if a change in security classification was warranted. Of all the Agency data, few data items were determined to be so sensitive as to justify access restrictions. The workgroup did identify drinking water well and intake locational information and detailed treatment process data as highly sensitive and worthy of additional restrictions. Other public water system facility locational data fields, such as treatment plant latitude/longitude coordinates, were not identified as highly sensitive.

Now, progress on source water assessments is generating new questions from our state partners concerning access to and display of information that EPA is collecting for delineated source water areas and related issues. States have raised concerns about the data handling procedures EPA has in place for storing the source water area and related assessment information. Several Regions and States believe the digital source water area polygons are of a sensitive nature and merit special handling procedures for the data. On the other hand, some states have decided to provide open access to their source water area information. Since this is a new data stream for EPA, voluntarily shared by the states with EPA, and because there is a wide variety of access and handling procedures for this data, OW included the SWAP data in the data fields considered as potentially sensitive in developing this information security policy.

Framework for Drinking Water Protection and Information Security

The Office of Water recognizes the importance of working with our state partners to reach consensus on how we handle the water data received from the states, as well as considering homeland security concerns. OW has developed this policy to balance security concerns and diverse state handling requirements with public health goals, right-to-know requirements, and other program and statutory responsibilities. OW recognizes that wide dissemination of information is critical for promoting local actions required to protect drinking water resources and that increased awareness, as in other security efforts, can increase security.

The drinking water program information elements included under this policy are:

- latitude and longitude coordinates of Public Water System (PWS) wells and intakes and GIS analyses derived from these data;
- delineated source water areas (SWA) and related State source water assessment program (SWAP) data available to EPA.

We considered, but (after much deliberation) decided against including in our policy the treatment plant location and treatment process information reported by the States into EPA's Safe Drinking Water Information System (SDWIS). Although OW has since 1998 restricted access to treatment plant latitude/longitude coordinates as equivalent to the restrictions on the intake and well coordinates, it is clear from our detailed review that the treatment plant location is generally available through other sources and in other forms. Continuing access restrictions to these data seemed inappropriate and ineffective. Although detailed treatment process information was identified as highly sensitive in our 2002 homeland security information reviews, the data reported to SDWIS is not detailed enough to trigger the need for access restrictions. We also have never placed access restrictions on this information in the past. The information provided to SDWIS is also available to the public from other non-EPA sources, including many utilities and states. Therefore, we have deleted both the treatment plant location and treatment process information from our final policy.

The access management strategy for these two remaining information categories is described in Table 1 and addresses use of Freedom of Information Act (FOIA) exemptions and other steps to manage the data, as well as the rationale for these measures. The approach to managing access to these two information categories is distinctly different:

- latitude and longitude co-ordinates of Public Water System (PWS) wells and intakes and GIS analyses derived from these data will be considered as potentially exempt from disclosure under FOIA Exemption 9 or other exemption categories in each case, as appropriate, based on homeland security considerations;
- delineated source water areas (SWA) and related State source water assessment program (SWAP) data available to EPA will be treated as sensitive for data management purposes and will be utilized for Federal purposes only under a special data handling protocol that specifies the conditions of their use.

OW is establishing further guidance on this policy in the form of Standard Operating Procedures (SOPs) which will follow from this policy and describe the detailed data handling procedures we will use. The procedures will be developed through a collaborative process with other EPA programs, the EPA Regions and the States. Through the SOPs, EPA will detail the access controls and handling procedures that will be put into place to protect these water data.

Thank you for your assistance in developing this "Policy to Manage Access to Sensitive Drinking Water-Related Information." We look forward to establishing with you and the States the aforementioned SOPs. To the extent that other drinking water information issues arise at the national level, we will work closely with the Regions and States to determine the best policy. OW believes that this balanced policy will promote protection of public health through the drinking water regulatory program and source water protection while enhancing the security of drinking water facilities.

Attachment

Attachment

Table 1
Management Strategy for Sensitive Drinking Water-Related Information

Data Category	OW Info Security Designation	Rationale/Explanatory Notes
1 - Latitude and longitude co-ordinates of Public Water System wells and intakes and GIS analyses derived from these data.	**OW considers this information highly sensitive and related to homeland security.** OW will limit public access consistent with Agency-wide sensitivity criteria to preserve authorized restrictions on information access and disclosure. Information systems and applications that access, store, or use this information will need to be modified to conform to this policy. OGWDW will consider withholding these data under FOIA Exemption 9 or other exemption categories as appropriate on a case by case basis.	o This information is not widely available. Unauthorized access to EPA's data could be misused for harmful purposes. o FOIA Exemption 9 is the most applicable authority for withholding this information because it specifically focuses on wells and, by inference, intakes. o OW will continue to exchange source water well and intake location data with our state co-regulators to allow updating but will follow the approved security plans and related procedures in response to all other requests for access. o To fully implement the integration measures of the Strategic Plan (measures 21-27), OW will share stream reach data with the States to verify the specific drinking water intake location on each NHD stream reach. o For public water systems that have reported the same latitude and longitude for both wells/intakes and treatment facilities, OW will treat both reported values as the locational information for wells/intakes and follow the processes above accordingly.
2 - Source water delineated areas (SWA) and related State source water assessment program (SWAP) data available to EPA	**Sensitive for data management purposes,** requiring special data handling procedures under an SOP applicable to all Federal users of the sensitive data. The SOP will require that specific protocols be followed before allowing general public access to the data. The SOP will also specify certain situations where EPA will treat the data as highly sensitive and consider bases for withholding information in response to specific requests for these data under FOIA.	OW does consider the source water area (SWA) polygon data it holds as sensitive for data management purposes because of differences in state handling requirements and because the SWA polygon data is derived directly from the source facility location. Special data handling procedures under an SOP will be required to access, store, and use all the SWA polygon data held by OW. As a general rule, OW will not deny access to the public on request. However, OW will treat the SWA polygon data as highly sensitive and will withhold data, based on applicable FOIA exemptions, where: o A State requests that EPA treat the data received from the state as confidential because the state has mandatory data access restrictions more stringent than EPA; or o EPA determines that the SWA geospatial representation could be used to identify the precise location of the intake or well.